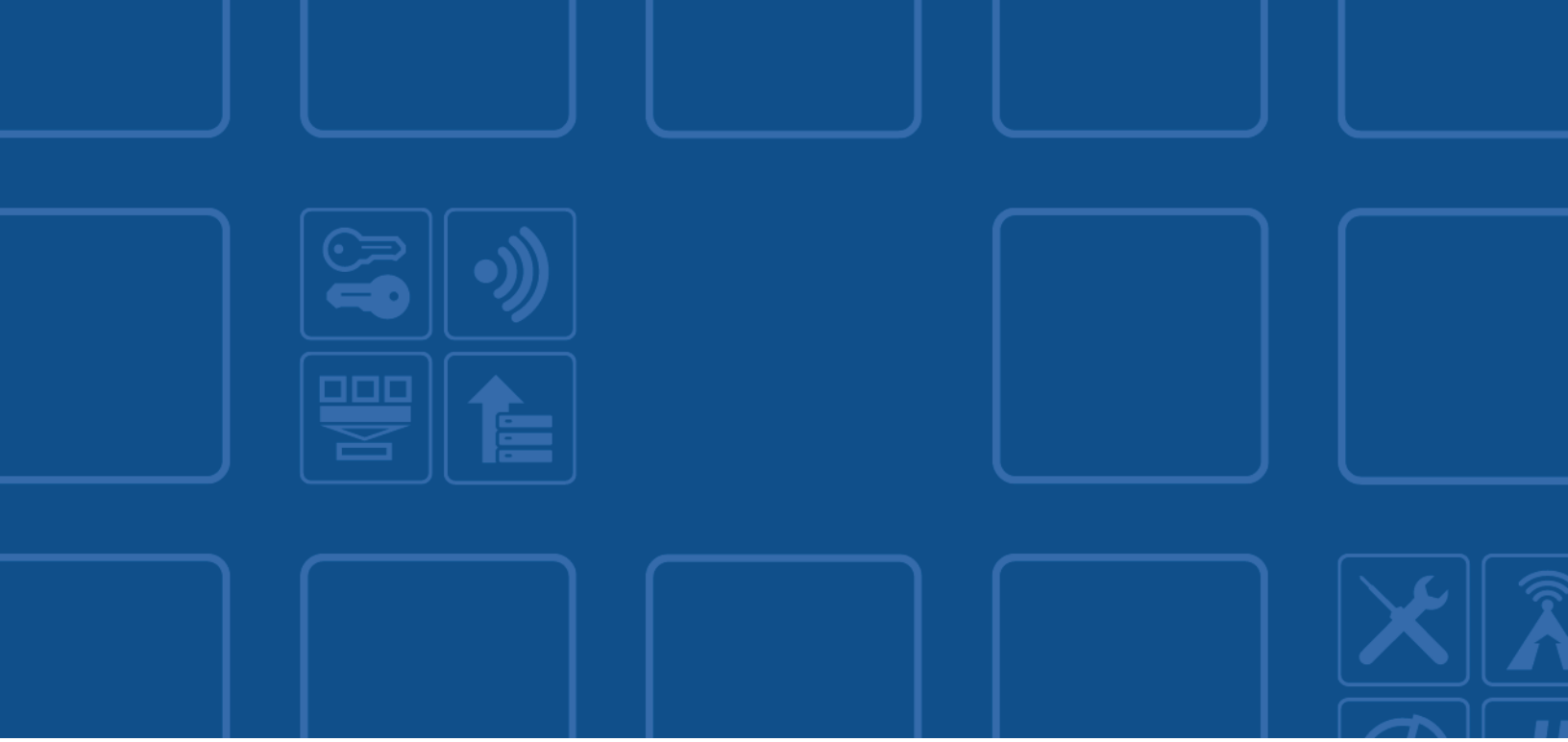
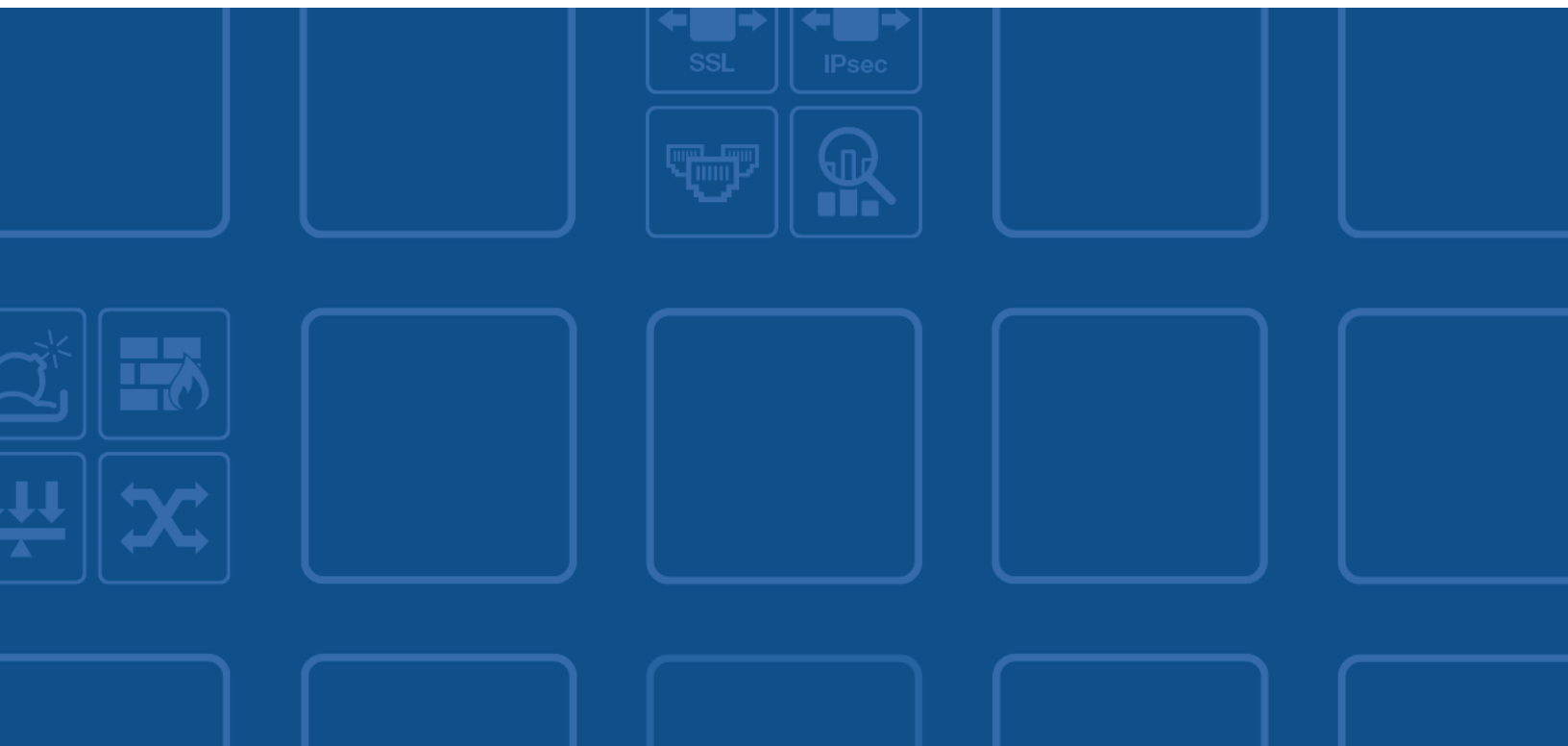


FORTINET
High Performance Network Security

FortiGate Connector for the HPE VAN SDN - Administration Guide

Version 1.1



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, May 24, 2016

FortiConnector for HPE VAN SDN Controller v.1.1- Administration Guide

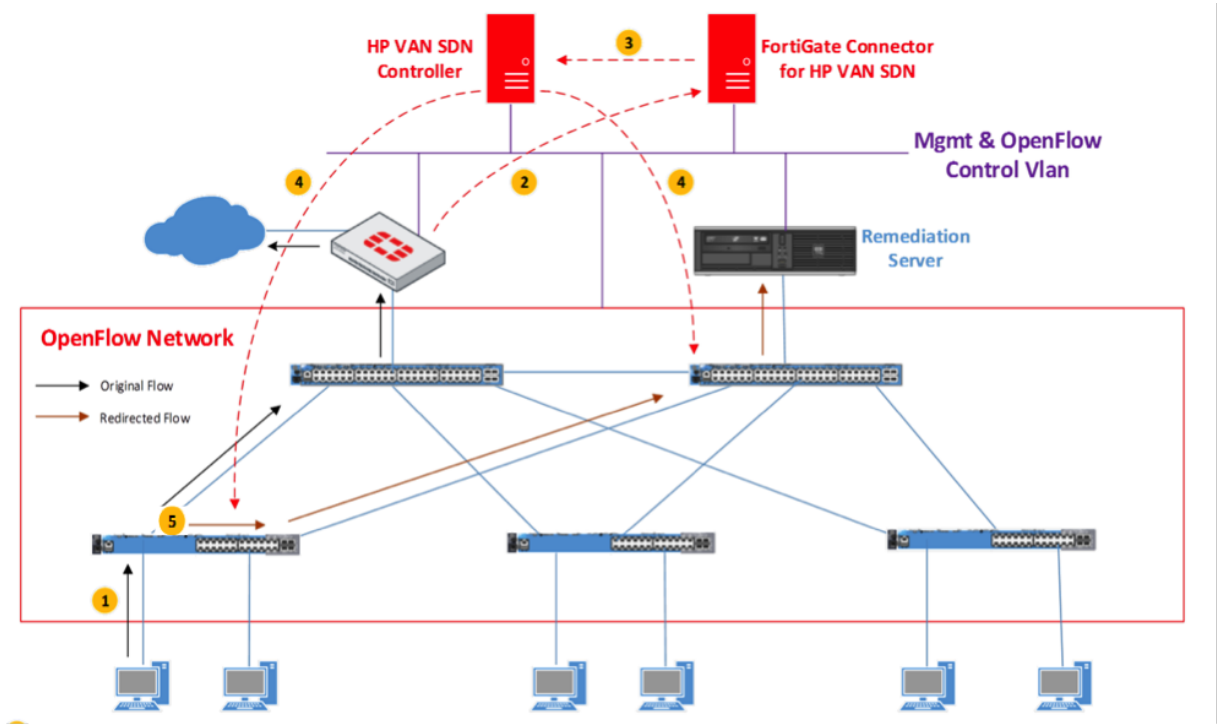
TABLE OF CONTENTS

Change Log

Date	Change Description
2016-05-13	Initial Release of v.1.1

Overview

FortiGate Connector for HPE VAN SDN is the Fortinet solution that provides preventive action or remediating action to a problematic endpoint causing security threats to the network. A preventive action isolates an endpoint from the rest of the network in case it generates malicious traffic such that from an exploit or from botnet command and control. The purpose of prevention is to block the user's traffic as close as possible to the connected switch and therefore prevent spread of attack to the rest of the network. A remediating action redirects the traffic of a problematic endpoint to a designated destination that acts as a remediation server. The server provides services to the endpoint such as antivirus database update and software patching. FortiGate Connector is also named as FortiConnector for short in documentation.



Number key for diagram:

1. Flow detection on FortiGate
2. FortiGate sends sys log message with 5-tuple of flow to FortiGate SDN Connector
3. FortiGate APP sends prevention action for this flow with 5-tuple through RESTful-API
4. Based on flow information and action type received from FortiGate Connector, HPE SDN Controller programs flow in HP OpenFlow switch through OpenFlow protocol with drop or redirection action.
5. Flow is blocked on HP switch port which the infected user is connected to, or redirected to a remediation server

In the products, HPE VAN SDN is also referred as HP VAN SDN, and FortiGate Connector as FortiConnector.

Licensing

FortiGate Connector for HP VAN SDN is free of charge for Fortinet customers. Your FortiGate must be registered with FortiCare at https://support.fortinet.com. Also, you will need to agree with the general Fortinet license agreement. The agreement can be found at http://www.fortinet.com/doc/legal/EULA.pdf.

Supported Products

FortiGate products

- All physical FortiGate devices running:
  - FortiOS 5.2
  - FortiOS 5.4
- A versions of FortiGate-VM running:
  - FortiOS 5.2
  - FortiOS 5.4

HP products

- HPE VAN SDN Controller version: 2.6.8
- HP Switch version: X.16.01.0004,
- HP Switch Models supporting prevention action: All switches of OpenFlow capability.
- HP Switch Models supporting remediation action: 2900 series, 3800 series.
- Some models of HP switches have limitation of remediation action. Please see release notes.

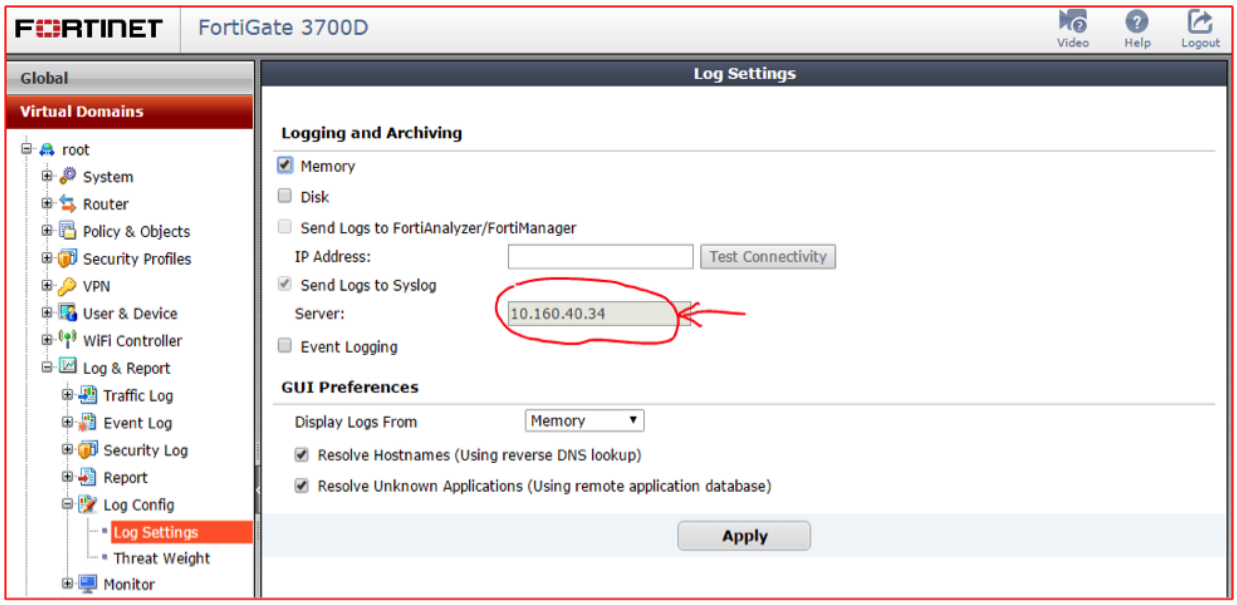
Features

The FortiGate Connector for HPE VAN SDN version 1.1 supports the following functions:

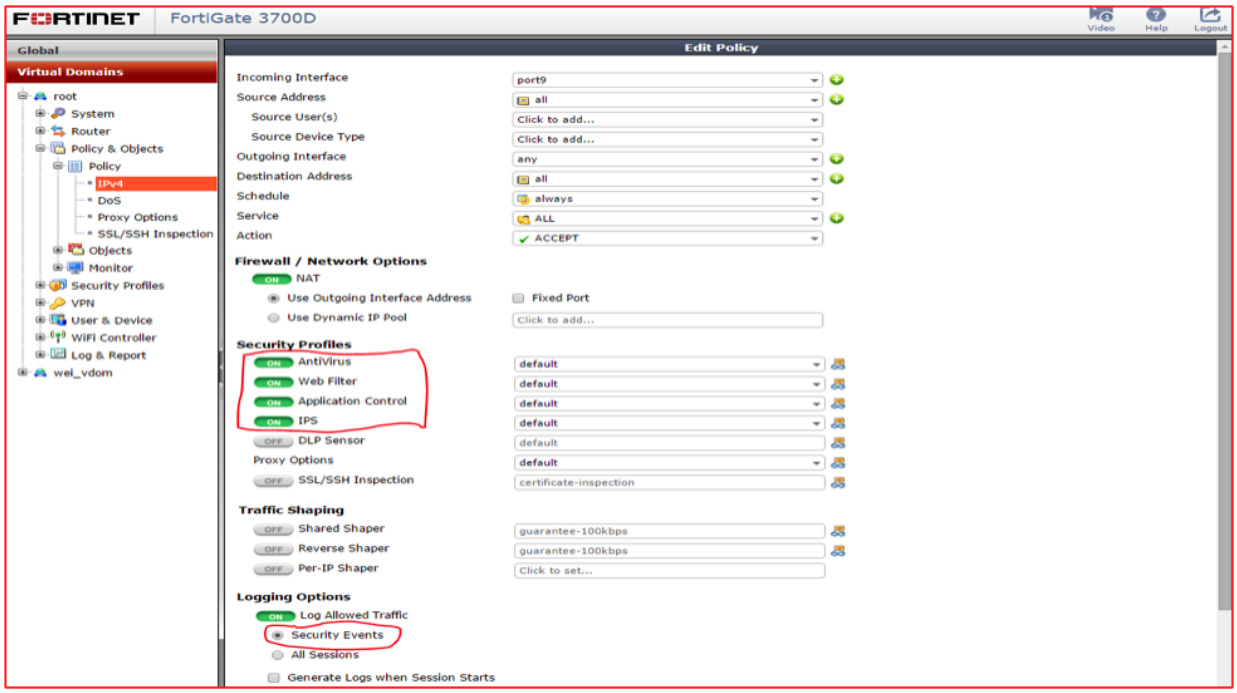
- Prevention or remediation action based on the results of scans by the AntiVirus engine.
- Prevention or remediation action based on the results of scans by the Intrusion Prevention System (IPS) engine.
- Prevention or remediation action based on scans set by parameters in the Application Control Profile.
- Prevention or remediation action based on scans set by parameters in the Web Filter Security Profile.

Prerequisites

- The FortiGate Connector IP address should be entered in the field for the Syslog server IP address on the FortiGate.



• In order for the FortiGate Connector to make use of the ***Security Profiles***, the profiles, as well as the ***Security Events*** option, need to be enabled on the FortiGate.



Installation

FortiGate Connector for HPE VAN SDN version 1.1 is packaged in two forms of release:

- Full package in a zip file that contains a VMware OVF release.
- Upgrade package in a zip file for directly upgrading FortiConnector version 1.0 systems to version 1.1.

The full package `FortiConnector-1.1.5-GA.zip` is released for a brand new installation. After the package is unzipped, VMware EXSi 5.5 or 6.0 should be used to install the OVF file with its relating files in the package.

If the upgrade package is going to be installed on the base of FortiConnector 1.0, a third party package must be installed first. The user can log in the console of the FortiConnector and issue the command:

```
sudo apt-get install apache2-utils
```

The upgrade package `FortiConnector-1.1.5-GA-upgrade.zip` can be deployed by the following procedure:

1. On the WEB interface, stop and clear the FortiConnector if it is running.
2. Login to the console of the FortiConnector with the root administrator credential.(default forticonnector/fortinet)
3. Stay in the FortiConnector home directory, install the third party package apache2-utils as above.
4. Rename the 'workspace' directory to a backup directory, e.g. type command: `mv workspace workspace-old`
5. FTP or SCP the upgrade package to the FortiConnector home directory.
6. Enter command: `install.sh FortiConnector-1.1.5-GA-upgrade.zip`
7. Refresh the WEB interface page and start using the new FortiConnector version.

Change Default root password

The default root credentials for FortiGate Connector for HP VAN SDN are:

- User name = `forticonnector`
- Password = `fortinet`

The user name cannot be changed but the password can be changed using the following steps:

1. Use the default root credentials to login to the FortiGate Connector.
2. At the prompt execute the following command:
   `passwd`
   The results will be:
   ```
   Changing password for forticonnector.
   (current) UNIX password:
   ```
3. Enter the current password which should be the default password `fortinet`.
   ```
   Enter new UNIX password:
   ```

4. Enter the new password that you want to use.
   `Retype new UNIX password:`
5. Verify the password by retyping it.If all done correctly the result should be:
   `passwd: password updated successfully`

Change default IP address

The default IP address is 192.168.1. 99

The IP address can be changed using the following command:

```
sudo ifconfig eth0 <new_IP_address> netmask <new_subnet_mask>
```

Change system time

FortiConnector's system time must be changed to the current time and should match that of the HPE VAN SDN Controller. It is strongly recommended network time protocol (NTP) server be used for time synchronization, by adding desired NTP server to the NTP configuration `/etc/ntp.conf` using an editor:

```
server <ntp_server_name_or_IP>
```

Restart the NTP by the command: `sudo service ntp restart`

Change default GUI management credential

The default login credentials of the GUI management interface are:

- User name = `admin`
- Password = `admin`

The user name and password can be changed using the following steps:

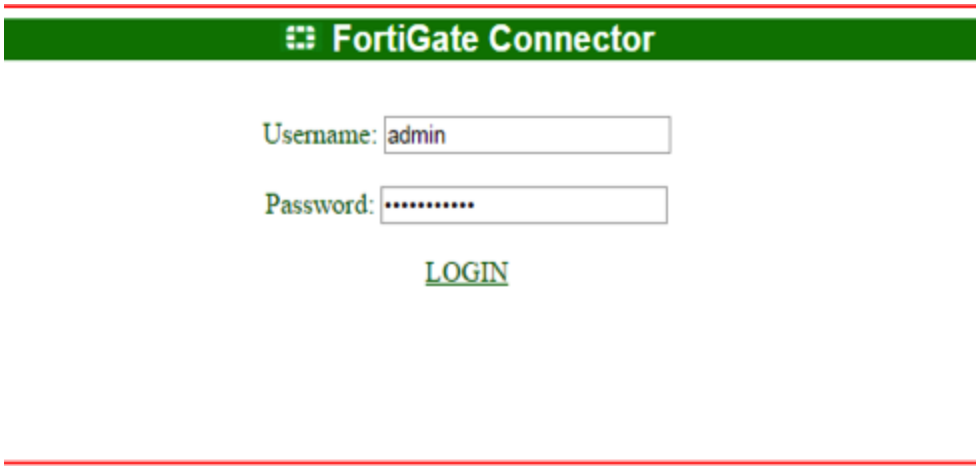
1. Login to the FortiConnector console with user name 'forticonnector' and its password.
2. Use the following command to change the password of the default user 'admin'
   `sudo htpasswd /etc/apache2/.htpasswd admin`

   Enter current password and then enter the new password.
3. If needed, a new user can be added
   `sudo htpasswd /etc/apache2/.htpasswd <new_username>`
   Then assign password to this new user.

It is strongly recommended that the default user admin's password be changed as early as possible.

Login Page

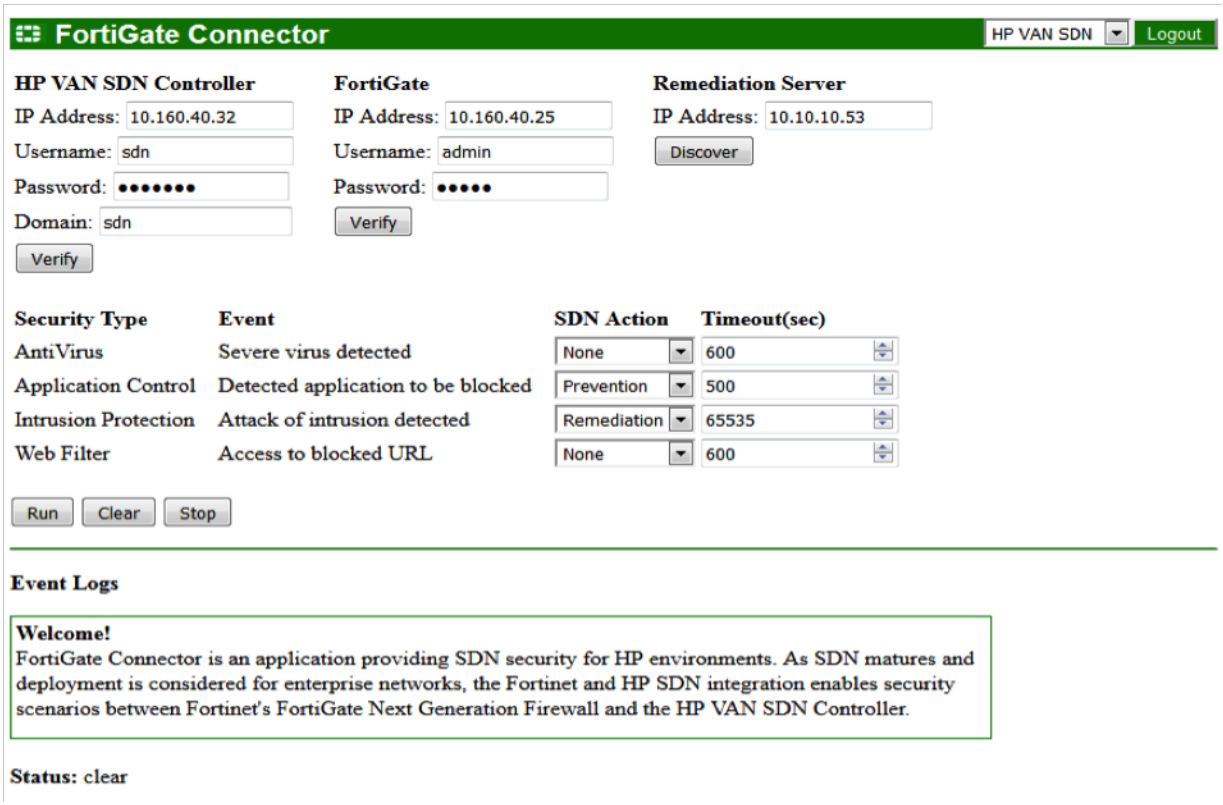
Logging into the GUI management interface is done by using the HTTPS prefix and the device's address in your browser as a URL. The default URL would be `https://192.168.1.99`. If the default IP address is still in use but your computer's address on a different subnet you will need to temporarily change the IP address of your computer to be on the same subnet.



Configuration Page

Once on the configuration page of the FortiGate Connector there are some configuration settings that may need to be changed to integrate the device and set the preferences for your network:

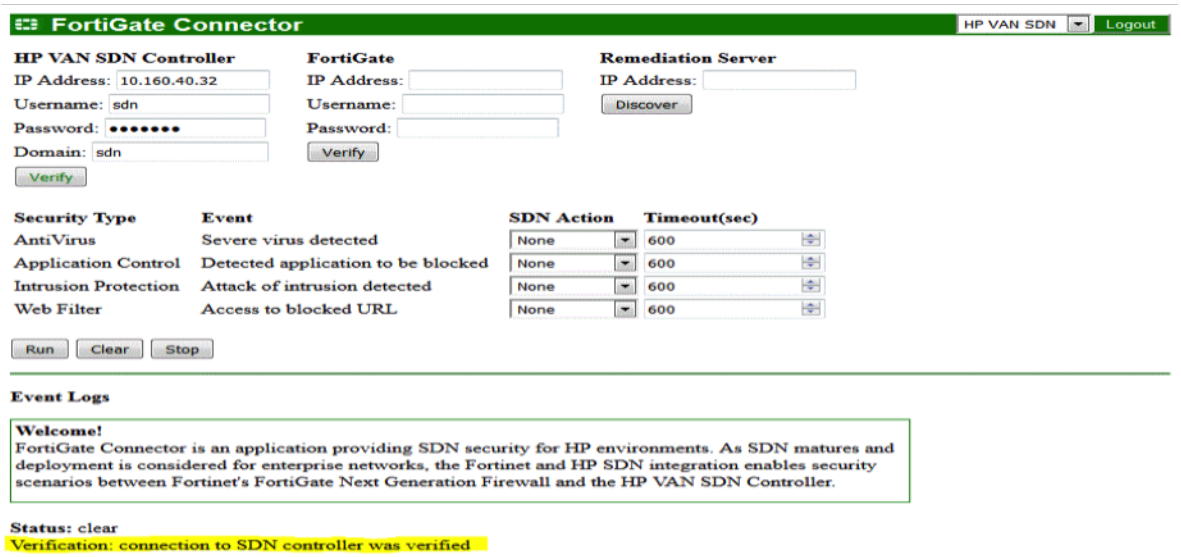
- Configure the IP address for the HP VAN SDN Controller, as well as access credentials.
- Configure the IP address for the FortiGate, as well as access credentials.
- Configure the IP address of the Remediation Server if remediation action is going to be selected.
- Configure Action type for each security type: None, Prevention, or Remediation.
- Configure flow timeout value for each security type. Enter 0 for no timeout given to the SDN controller.

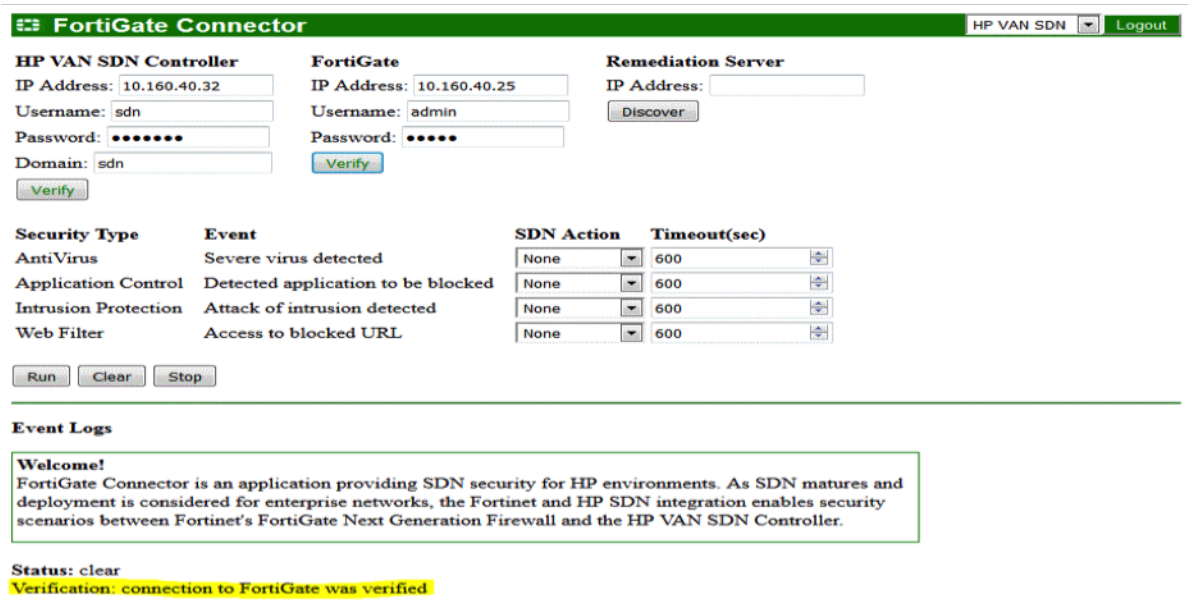


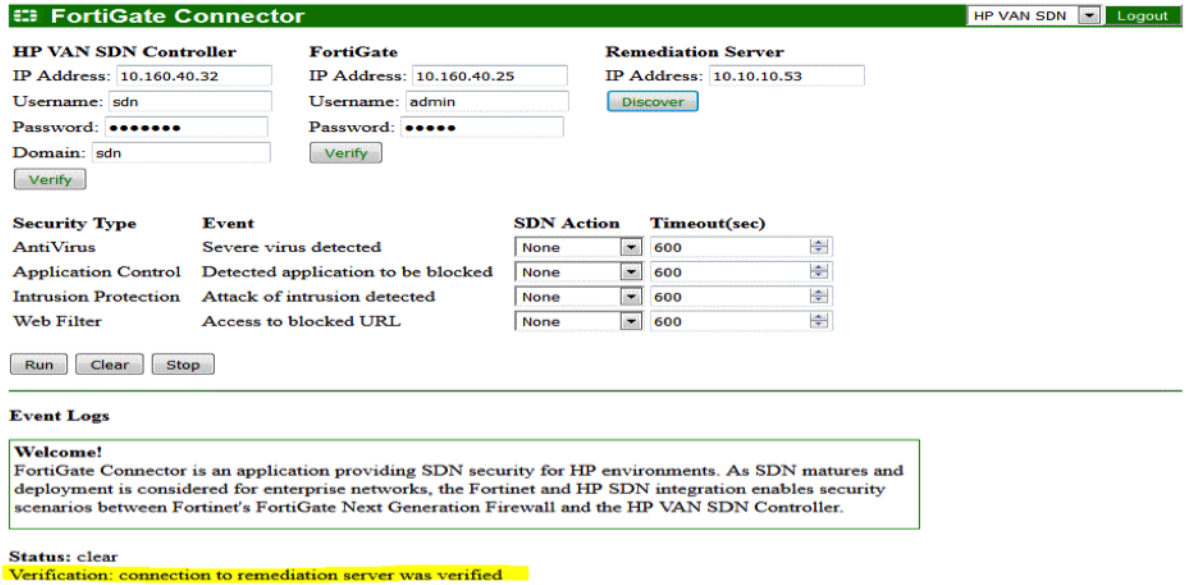
Authentication verification and connectivity discovery

Before starting FortiConnector, a user can click the “Verify” button to verify its authorized connectivity to the HP VAN SDN Controller and the FortiGate respectively. The “Discover” button of Remediation Server will work only If one or more remediation action is turned on, the failure of Remediation server discovery may bring user’s attention to trouble shooting the issue (A recommendation is that the user manually generate traffic from Remediation server to trigger that SDN controller learns Remediation server; user needs to click “Discover” button again to make sure the discover button in green state.). If verification or discovery is successful, the result is displayed in the footnote area under status, and the corresponding Verify/Discover button becomes green color. Otherwise, an error message shows under “Status:” and “Verify” button and “Discover” button are in red state.

When FortiConnector is running, configuration changes of SDN, Fortigate and Remediation server won’t take effect and “Verify” and “Discover” buttons are not function, until the FortiConnector is stopped and run again.

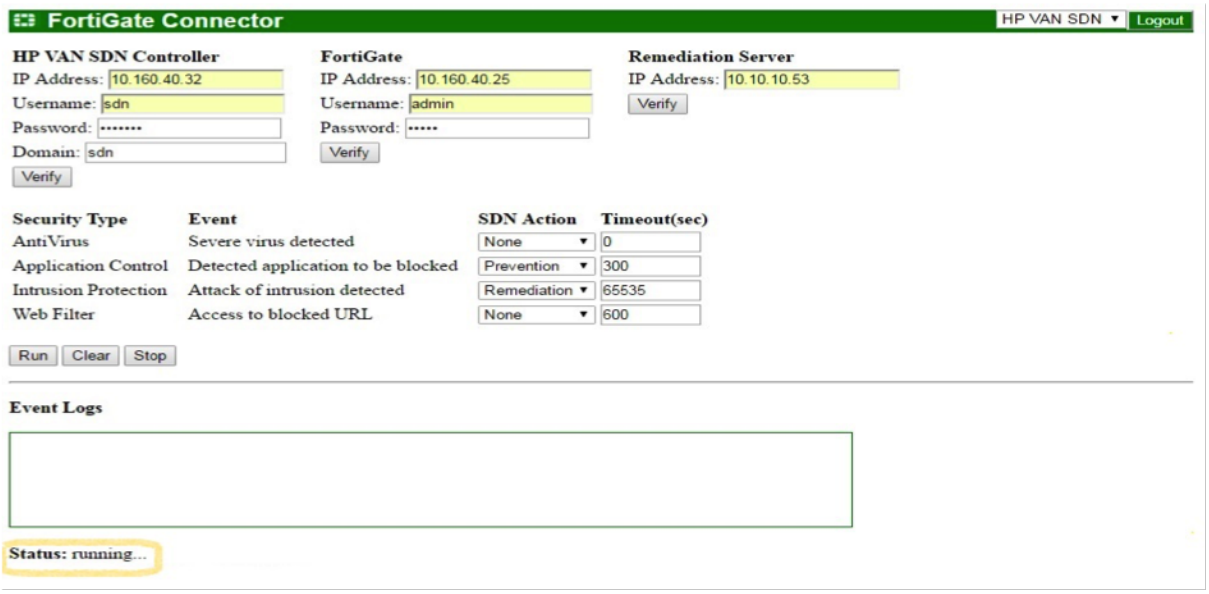

FortiGate Connector
HP VAN SDN
Logout
HP VAN SDN Controller
IP Address: 10.160.40.32
Username: sdn
Password: •••••••
Domain: sdn
Verify
FortiGate
IP Address:
Username:
Password:
Verify
Remediation Server
IP Address:
Discover
Security Type
Event
SDN Action
Timeout(sec)
AntiVirus
Severe virus detected
None
600
Application Control
Detected application to be blocked
None
600
Intrusion Protection
Attack of intrusion detected
None
600
Web Filter
Access to blocked URL
None
600
Run
Clear
Stop
Event Logs
Welcome!
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.
Status: clear
Verification: connection to SDN controller was verified


FortiGate Connector
HP VAN SDN
Logout
HP VAN SDN Controller
IP Address: 10.160.40.32
Username: sdn
Password: •••••••
Domain: sdn
Verify
FortiGate
IP Address: 10.160.40.25
Username: admin
Password: •••••
Verify
Remediation Server
IP Address:
Discover
Security Type
Event
SDN Action
Timeout(sec)
AntiVirus
Severe virus detected
None
600
Application Control
Detected application to be blocked
None
600
Intrusion Protection
Attack of intrusion detected
None
600
Web Filter
Access to blocked URL
None
600
Run
Clear
Stop
Event Logs
Welcome!
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.
Status: clear
Verification: connection to FortiGate was verified



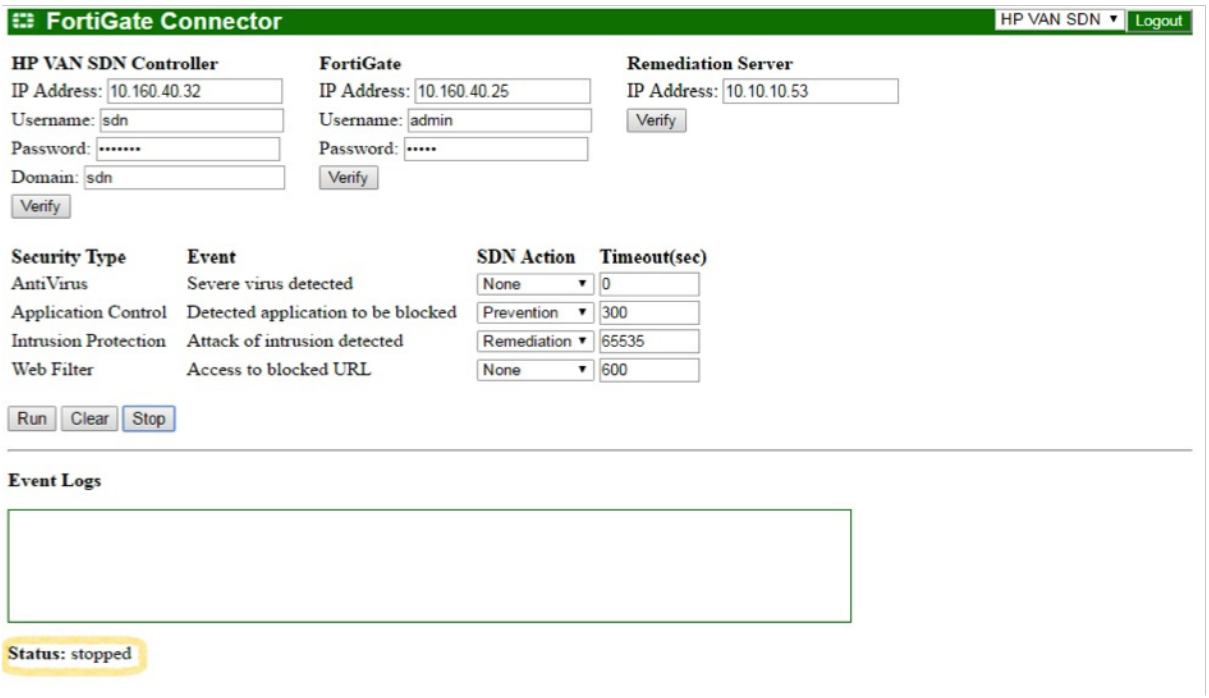
Starting the FortiGate Connector

Once the correct settings have been configured select the ***Run*** button.The application should start. When the ***Status*** indictor displays "***running ...***", it means the FortiGate Connector is ready to receive Syslog information from the FortiGate and to push the flows to the HP VAN SDN Controller.



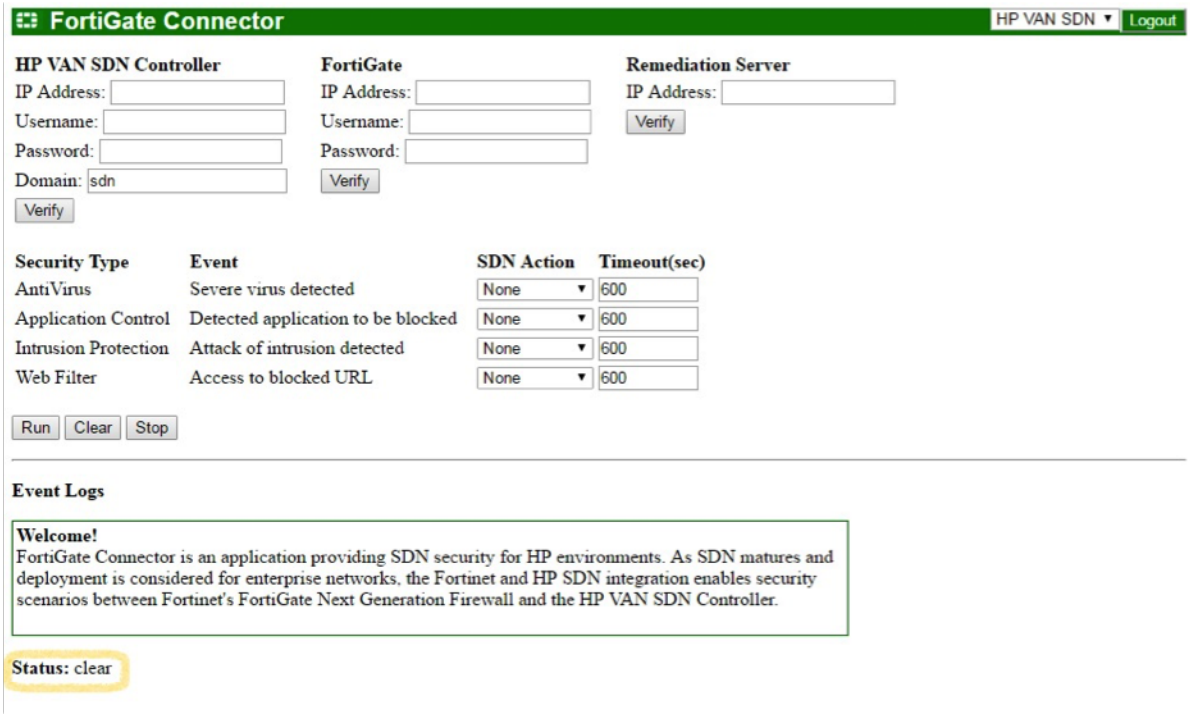
Stopping the FortiGate Connector

To stop the FortiGate Connector, select the ***Stop*** button. The ***Status*** indicator will display "***stopped***".This means FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, but the all the configurations are unchanged and maintained.



Clear the configuration and stop FortiGate Connector

To clear the FortiGate Controller, select the ***Clear*** button.The application will stop and configurations will be cleared. When the ***Status*** indicator displays "***clearing…stopped***", it means the FortiGate Connector has stopped all previously pushed flows from being sent to the HP VAN SDN Controller, and has cleared previous configurations.


FortiGate Connector
HP VAN SDN
Logout
HP VAN SDN Controller
IP Address:
Username:
Password:
Domain: sdn
Verify
FortiGate
IP Address:
Username:
Password:
Verify
Remediation Server
IP Address:
Verify
Security Type
Event
SDN Action
Timeout(sec)
AntiVirus
Severe virus detected
None
600
Application Control
Detected application to be blocked
None
600
Intrusion Protection
Attack of intrusion detected
None
600
Web Filter
Access to blocked URL
None
600
Run
Clear
Stop
Event Logs
Welcome!
FortiGate Connector is an application providing SDN security for HP environments. As SDN matures and deployment is considered for enterprise networks, the Fortinet and HP SDN integration enables security scenarios between Fortinet's FortiGate Next Generation Firewall and the HP VAN SDN Controller.
Status: clear

Supported use scenarios

Prevention scenarios

- When a user sends a malware file through the network and the FortiGate detects it, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a block action, to the HP SDN controller. The user port of the HP switch will then block all subsequent traffic from this user's IP address.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the listening port number, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all matching application traffic from this user's IP address. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a block action command to the HP SDN controller. The user port of the HP switch then blocks all traffic from the user's IP address to the website's IP address. Traffic from the user to other websites is not affected.

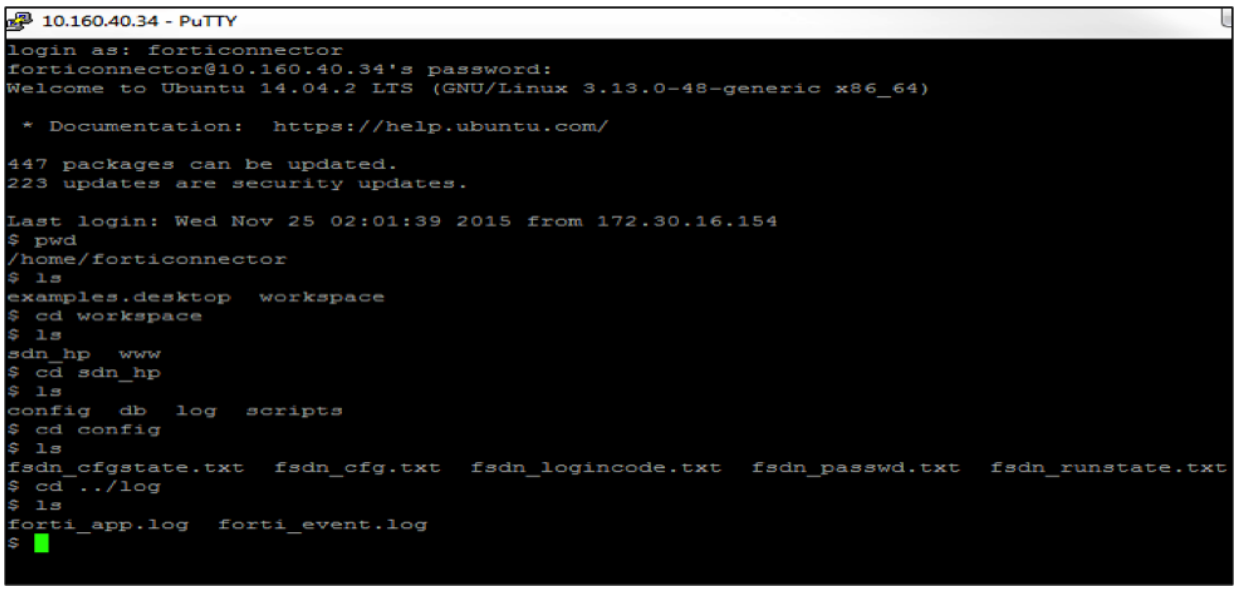
Remediation scenarios

- When a user email containing an attachment of computer virus is sent though the network and detected by the FortiGate, the FortiGate Connector will push the flow, along with user host’s source IP address and a redirect action, to the HP SDN controller. The user’s subsequent traffic of the source IP will be redirected to the remediation server for corresponding antivirus handling.
- When a user generates a botnet command to attack the network that is detected by the FortiGate IPS engine, the FortiGate Connector will push the flow, along with the user's source IP address and a redirect action, to the HP SDN controller. The user’s traffic from the same source IP will be redirected by the HP switch to the remediation server, which enforces a designated policy on the user.
- When a user initiates an application prohibited by the Application Control profile on the FortiGate, the FortiGate Connector will push this application flow, along with the user's source IP address, the destination IP address, the destination port number, and a redirect action command to the HP SDN controller. The HP switch then redirect all matching application traffic from this user's IP address to the remediation server for designated action. Other traffic from the user is not affected.
- When a user tries to access a web site prohibited by the FortiGate's Web Filter profile, the FortiGate Connector will push this web access flow, along with the user's source IP address, the destination IP address of the web site, and a redirect action command to the HP SDN controller. The HP switch then redirect all traffic from the user's IP address to the website's IP address instead to the remediation server for web filtering handling. Traffic from the user to other websites is not affected.

Basic Troubleshooting

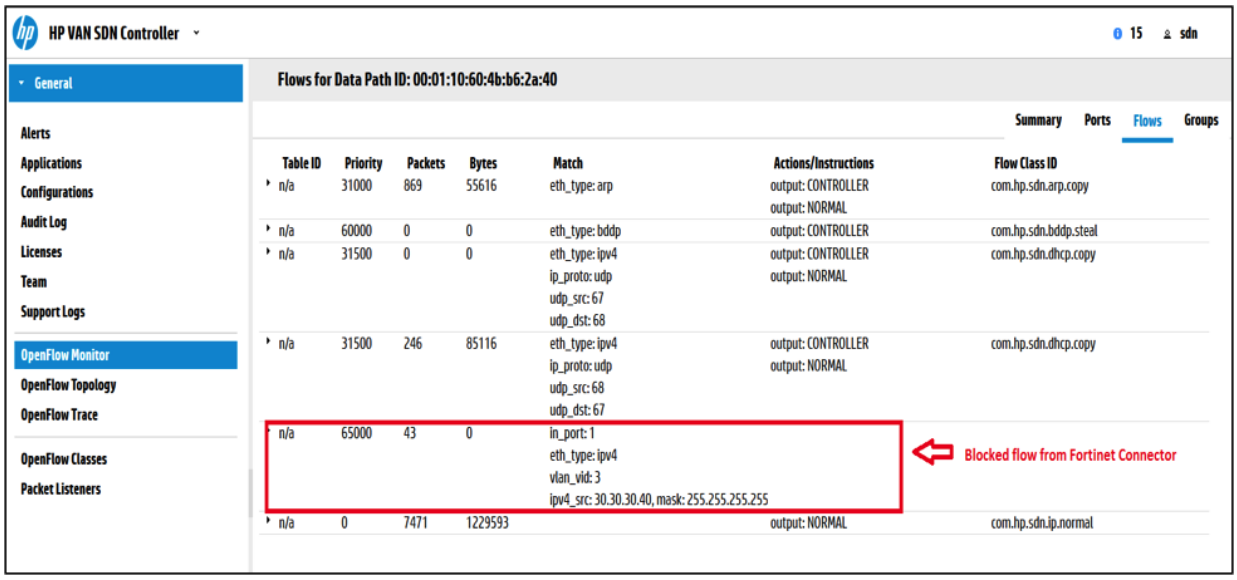
The following are some quick pieces of information that may be helpful in troubleshooting issues that may come up while administering your FortiGate Connector:

- The configuration file is located in the folder: `/home/forticonnector/workspace/sdn_hp/config/`
  - The file is: `fsdn_cfg.txt`.
- Debug messages and event logs are located in the following files:
  - `forti_app.log`
  - `forti_envent.log` (contains events only)
- The syslog messages from the FortiGate are located in the folder: `/var/log/syslog`.



Verify flow pushed by FortiGate Connector on HP SDN Controller for prevention

In order to verify flows pushed by the FortiGate Connector to the HPE VAN SDN Controller, navigate to the flow page on the HPE VAN SDN Controller.

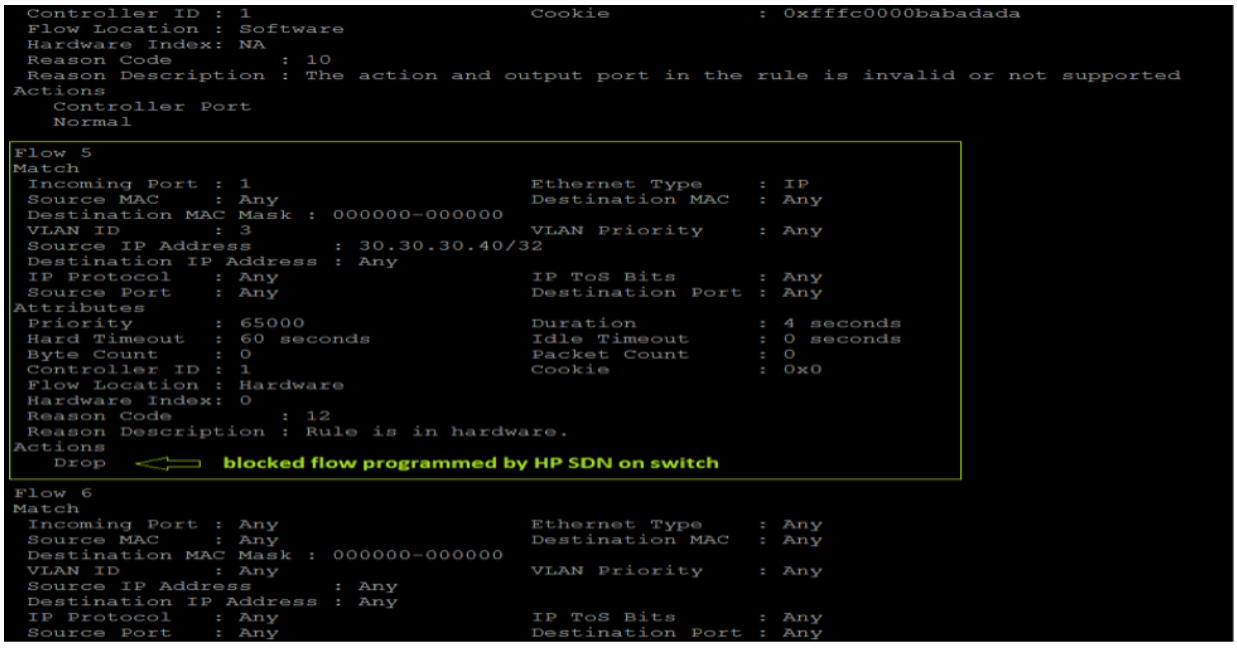


Verify flow pushed by FortiGate Connector on HP switch for prevention

In order to verify flows pushed by the FortiGate Connector to the HP Switch

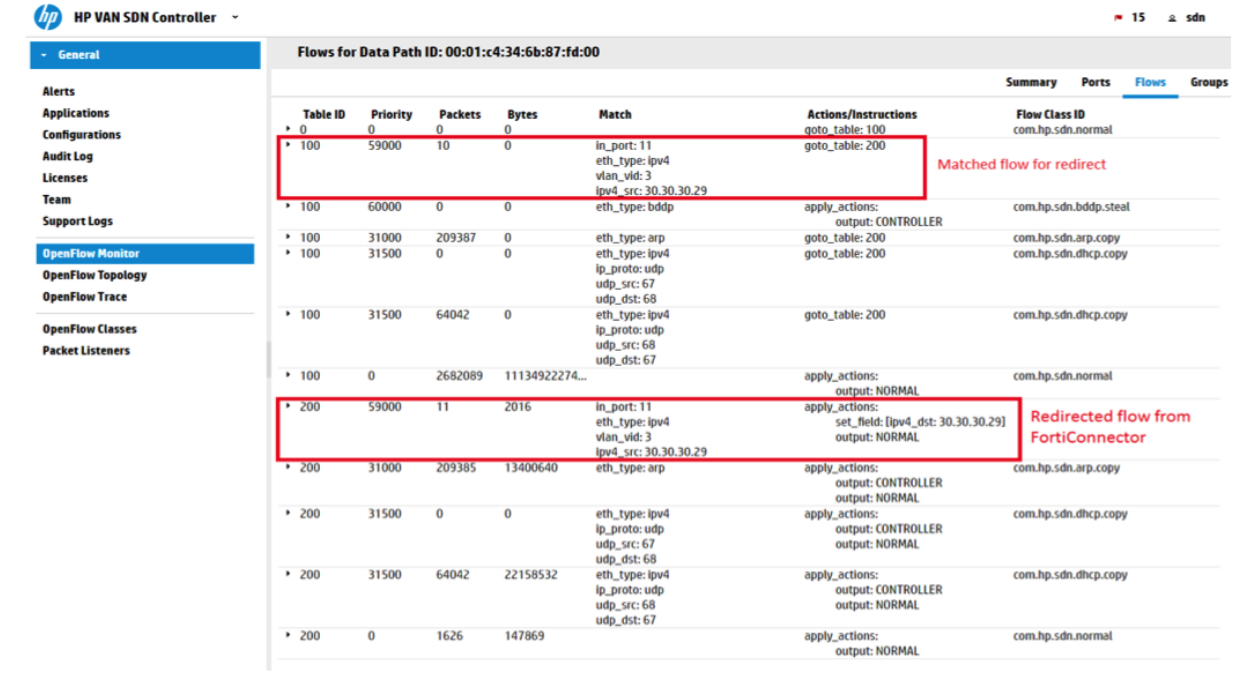
1. Login to the HP switch console.
2. Issue the following command:

```
HP-Switch# show openflow instance aggregate flows
```



Verify flow pushed by FortiGate Connector on HP SDN Controller for remediation

In order to verify flows pushed by the FortiGate Connector to the HPE VAN SDN Controller for remediation action, navigate to the flow page on the HPE VAN SDN Controller. The flow matched by the remediation action for redirecting to remediation server can be observed, if the flow was pushed from the FortiGate Connector correctly.

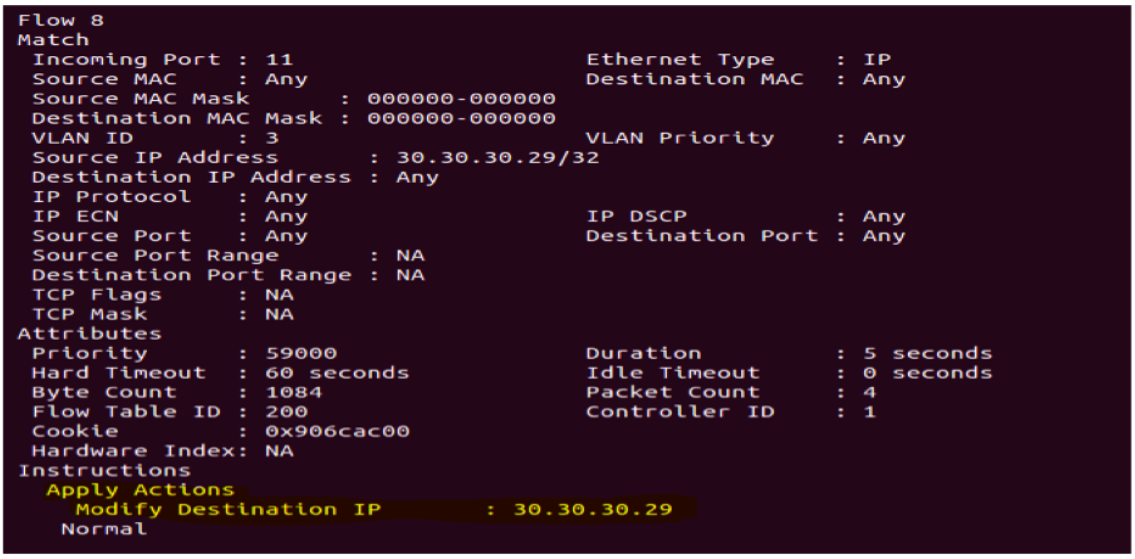


Verify flow pushed by FortiGate Connector on HP switch for remediation

In order to verify flows pushed by the FortiGate Connector to the HP Switch for remediation action:

1. Login to the HP switch console.
2. Issue the following command:

```
HP-Switch# show openflow instance aggregate flows
```


Flow 8
Match
Incoming Port : 11
Ethernet Type : IP
Source MAC : Any
Destination MAC : Any
Source MAC Mask : 000000-000000
Destination MAC Mask : 000000-000000
VLAN ID : 3
VLAN Priority : Any
Source IP Address : 30.30.30.29/32
Destination IP Address : Any
IP Protocol : Any
IP ECN : Any
IP DSCP : Any
Source Port : Any
Destination Port : Any
Source Port Range : NA
Destination Port Range : NA
TCP Flags : NA
TCP Mask : NA
Attributes
Priority : 59000
Duration : 5 seconds
Hard Timeout : 60 seconds
Idle Timeout : 0 seconds
Byte Count : 1084
Packet Count : 4
Flow Table ID : 200
Controller ID : 1
Cookie : 0x906cac00
Hardware Index: NA
Instructions
Apply Actions
Modify Destination IP : 30.30.30.29
Normal

FORTINET®

High Performance Network Security